Utilizing Ingress as a Plant Maintenance Strategy

Raymond J. Schneider

A new concept is described which uses a transmitter located in the return path frequency interval to ingress coded signals into the system. A vehicle equipped with a GPS, a leakage detection system and a transmitter sends information, via coded ingression, back to a monitoring device at the head-end creating a centralized leakage and ingress database as a by-product of the maintenance cycle.

We describe a prototype system used to test out these concepts. Data is presented on a small model cable system used to initially prove out the system. More definitive data will be developed on a portion of the Time Warner system in Harrisonburg.

THE PROBLEM SUMMARY

Situation

Ingress is a particularly difficult problem in the return path frequency interval due to the many signal sources that exist below 45 MHz and other factors. This is particularly troublesome since the return path is becoming increasingly important as the vehicle for various bi-directional interactive services such as Internet access.

Problem Components

Both the leakage and ingress problem have common components. The problem generally arises from weaknesses in the rf shield integrity. These weaknesses create points at which egress, usually called leakage, and ingress can occur. At these weaknesses rf energy can leave or enter the system much more readily than when the shield integrity is intact.

The problem is to detect, classify and localize the leakage or ingress energies so that the weaknesses can be found, diagnosed, and corrected. Leakage is found by driving through the system, however, ingress has been primarily investigated by performing spectral analysis on the return path signals at the head-end. This analysis can be effective for detection and classification, but is of little use for localization.

Current Response

The primary response to both FCC regulation and dealing with system ingress in both the upstream and downstream legs of the system has been a pro-active leakage and system integrity program. This requires systems to perform rf leakage surveys on a continuing basis to detect, classify, localize and correct defects. The detection of leakage energy is accomplished by traversing the system with sensitive leakage detection receivers which listen for emissions from the system.

To ensure that detected emissions are actually from the system, the transmissions use specially modulated coded signals such as the Sniffer transmitter or tagging signals applied to normal downstream traffic.

Deficiencies In the Current Response

This response requires specially trained technical personnel to conduct surveillance of the system on a quasi-continuous basis. The localization of defects is uncertain, due to a number of factors. Such factors include the tendency of rf leakage energy to reach the surveillance receiver by a combination of multi-path and direct path, standing waves on the

sheath of the transmission system, intermittency and others.

A *find and repair* sequence is both time consuming and expensive, so it is quite common to separate the functions of surveillance and repair, logging the leakage during surveillance and returning to logged leakage sites to repair the system. Leaks are seldom entirely stable. One must return to the surveyed site and re-detect, localize, diagnose and then repair the defects.

Surveillance Automation

A partial solution is to automate the surveillance process. ComSonics and others have developed leakage detection and logging systems which combine leakage information with GPS (Global Positioning System) information. Figure 1 illustrates this kind of system diagramatically.

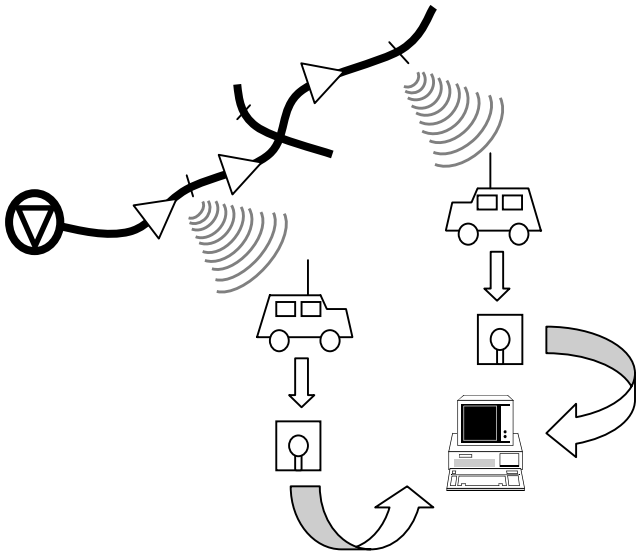

Figure 1. Typical Leakage Surveillance System

The principle advantage of this method is that it provides dense coverage with very little operator intervention. System coverage can be total and nearly continuous if there are sufficient vehicles instrumented and they drive through the system on a regular basis. A disadvantage is the manual process of handling the diskettes generated by several vehicles, and the time required for the associated processing.

Once the data has been processed, it is a relatively simple matter to generate work orders to service the hot spots in the system. A difficulty at this point is that the data is collected as latitude/longitude data and must be processed to produce actual street addresses. This processing requires a current map base that is as accurate as the GPS. Then, for each leak listed on the work order, a cable service person must re-localize, diagnose and fix the leak.

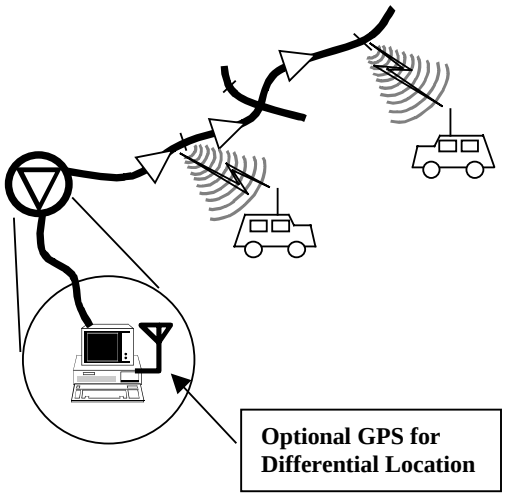

Figure 2. Diagram of the Ingressor Concept

A NEW CONCEPT

We have been working on a new concept which solves the majority of the problems with the mobile data logging approach. In addition, the concept offers new and interesting capabilities.

Figure 2 illustrates what we call the Ingressor Concept. In this concept the leakage monitoring vehicle does not log the data to a disk or other on-board storage media (although this capability would still exist as a backup). Instead, the system transmits position and leakage information which can be gathered at a central point either by direct path reception or, perhaps not as obvious, by receiving the signal via the ingress path.

The Conceptual Components

The Ingressor Concept has several conceptual components:

1. The primary signal is provided by ingress using a coded broadcast in the return path frequency interval of the cable system;

2. The surveillance vehicle transmits the signal which ingresses into the cable system as a function of the path of the vehicle, the location of the cable plant relative to the vehicle, and the relative shielding effectiveness of the portion of the plant closest to the vehicle;

3. On the transmitted signal is impressed both GPS position data for the vehicle and leakage (egress) data detected from the vehicle;

4. At the head-end, a receiver detects the presence of the ingression at the selected frequency, decodes the GPS and leakage information, and measures the signal strength of the received transmission;

5. If a map of the system is available, the system processes the data to produce a running measure of the shielding effectiveness along the plant strand map;

6. Peaks in the received ingress signal are correlated with peaks in the transmitted leakage information and the position of the leak is inferred more accurately than from leakage alone;

Figure 3. The single span model system

7. If differential GPS is used together with a surveyed plant map, the location of points of leakage or weak shielding effectiveness can be located with an accuracy on the order of 5 meters. (Single station GPS accuracy is only 100 meters.)

8. The same system which processes the received ingression signal can also be equipped to perform spectral analysis of the entire return path frequency bandwidth.

Using the GPS timing signals to synchronize the transmissions, a TDMA (Time Division Multiplex Approach) can be implemented. This allows multiple vehicles to share the same frequency and intermix their signals, so that far more coverage efficiency is

achieved than if the system were restricted to a single vehicle.

PROTOTYPING THE CONCEPT

To determine if the Ingressor concept was viable, we decided to build a prototype system in two phases. The first phase was to develop a hardware prototype and test it on a miniature cable system built at ComSonics for this purpose. Once the prototype is shown to be functional on this system, it will be migrated to the local Time Warner cable system in Harrisonburg, VA and tested on that system's return path. This second phase will allow both higher fidelity and a much larger range of geometries and leaks to be evaluated.

The Model System

Figure 3 depicts the model system. It consists of a single short 20' span of cable with a trunk bridger, a line extender and a splice block mounted between two support poles. The model system is fed from an equipment rack inside the ComSonics building. For the data shown here, the only signal on the system was a Sniffer transmitter on 108.625 MHz. The ingress transmitter is mounted together with a GeoSniffer system equipped with a ComSonics Sleuth leakage detection receiver in a vehicle. The transmitter is a Motorola Radius low band transceiver transmitting a measured 47 watts into a 5/8 wavelength whip at 27.47 MHz.

Preliminary Data Runs

Figures 4, 5 and 6 depict ingress/leakage runs past the model system under three different conditions:

- a run past the model system with the system totally sealed (Figure 4)
- a run after a small leak (approximately 45 μV/m at 10 feet) has been introduced into the system (Figure 5)
- a run after a larger leak (approximately 190 μV/m at 10 feet) has been introduced into the system (Figure 6)

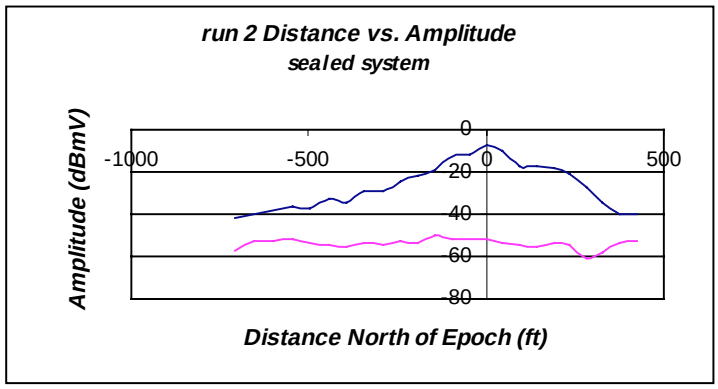

Figure 4. A run past the model system sealed

The output of the GeoSniffer was connected to a modem and a digital data stream transmitted. The data consisted of the GPS position updates once a second, and the Sleuth leakage data at the time of the GPS update. The data was burst transmitted at a fixed time offset relative to the GPS clock. A receiver connected to the model system looked for the signal and if present synced with it and read the information. In addition to reading the GPS and Sleuth information the system recorded the AGC and RSSI (log output) voltages from the receiver. This data was used to create a calibration table for estimating the amplitude of the incoming ingression signal. Since this is early in our experiment, the errors are not perfectly understood. We believe the data is accurate to about 3 dB.

Data Interpretation

The data depicted in Figures 4, 5, and 6 shows both the ingress and leakage data plotted against distance relative to epoch. The term *epoch* is used to denote that point which has the

largest ingress amplitude as the vehicle passes the model system. This point will be near the system, but not necessarily exactly when the vehicle passes closest to the system.

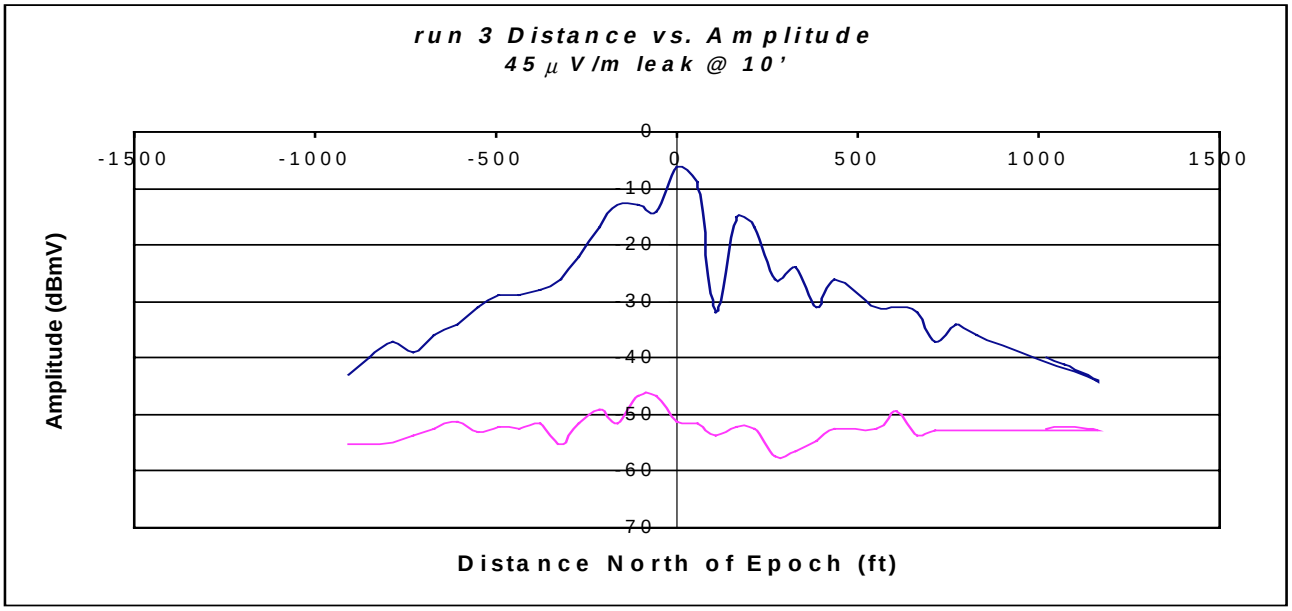

Figure 5. A run past a small (45μV/m) leak

The distance is calculated by differencing the epoch location from the latitude and longitude of the data points and converting the difference to a distance in feet. Distance which is relatively North of the epoch is designated as positive, and distance South of the epoch is designated as negative. If the epoch were exactly abreast of the model system, it would be approximately 100' from the first pole.

The data is displayed from South to North. In each data plot, the top trace is the ingress data and the bottom trace is the leakage data. The model system is on the South side of the ComSonics building offset about twenty feet.

Fully Sealed System

The first thing to note is that one only gets information from the system when the ingress is present and at a signal to noise level sufficient to read the data reliably. This level is nominally –35 dBmV. In run 2 depicted in Figure 4, the system reliably ingressed from about 700' South and closer. Notice that the signal intensity grows steadily to the epoch and then declines and there are only slight ripples in the data. The associated leakage data shows no sign of peaking.

A Small Leak

At least three effects different from the sealed system run are apparent in the data from the small leak run (run 3). These are:

- The signal dropped out at 900'-1000' instead of 700' from the epoch.

- The leakage data shows a noticeable peak just prior to the epoch indicating that the leak is being detected.

- There are several major swings in signal amplitude after passing the epoch to the North.

We currently believe that the peak in the leakage data occurs approximately when we are abreast of the model system. The large swings are believed to be due to multipath, an interfering reflection from the metal side of the ComSonics building which goes in and out of phase as the vehicle proceeds North. About three cycles of declining amplitude can be seen in the data of Figure 5.

A Larger Leak

Introduction of larger leaks in the model system created stability problems with the prototype. The initial effort to create a larger leak produced data which contained spikes and oscillations. To correct this problem we inserted a 20 dB attenuator at the input to the receiver. Run 6, depicted in Figure 6 shows the result when we drove past the system with a 190 µV/m leak. Even with a 20 dB attenuation, the receiver began to receive and decode usable data at a range of between 1414' to 1486' feet from the model system on this run.

The same kinds of features are observed on this run as on the low leakage run. The first ingression peak correlates with the first leakage peak.

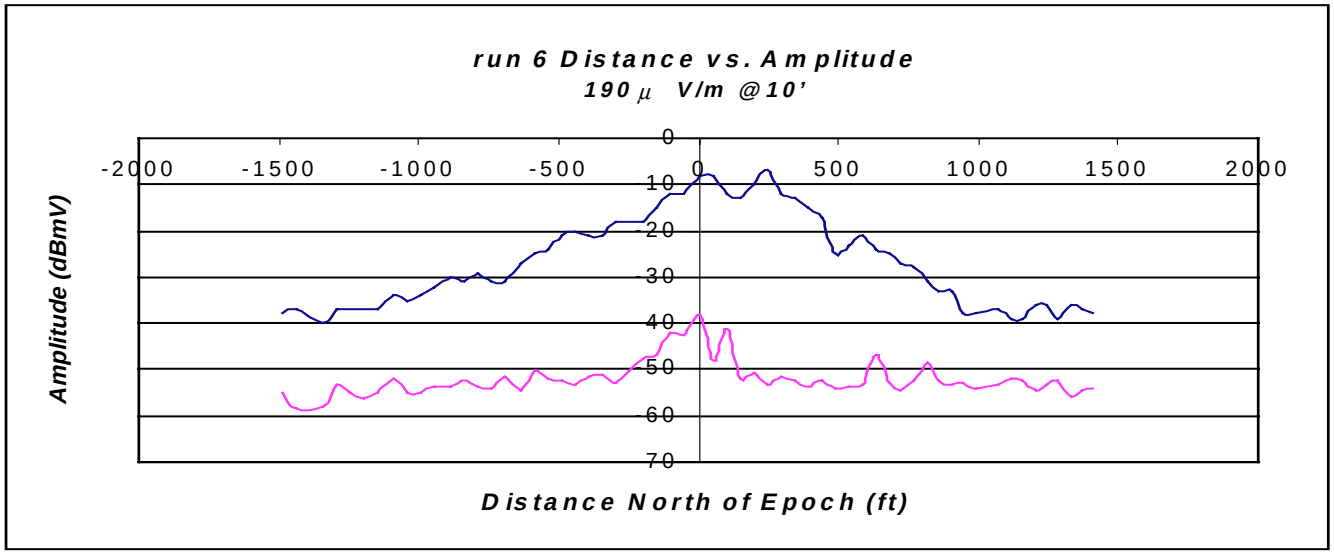

Figure 6. A run past a larger (190µV/m) leak

Conclusions

Ingression occurs into a sealed system from distances on the order of 700' with 47 Watts of radiated power, such that coded digital data can be extracted. Even a small leak increases this range by about 30%. A larger leak increases this range by over 100% to in excess of 1400'.

The fact that ingress is so readily achieved allows it to be used as an unorthodox but highly diagnostic data path to the headend.

Combining leakage and ingression data gives additional information which supports better leak/ingress position determination.

Structure in the ingress amplitude allows intelligence about the state of the cable system to be extracted.

Lower power than employed in this test will still routinely ingress data into the cable system. Optimum power levels will be studied in phase two of this work.

Acknowledgements

I would like to take this opportunity to thank Dennis Zimmerman, the CEO of ComSonics who had the original idea for the Ingressor Concept. There is a patent currently pending. I would further like to thank Randy Smith, whose hard work made it possible to collect this data.

Raymond J. Schneider
Director of Engineering
ComSonics Inc.
1350 Port Republic Rd.
Harrisonburg, VA 22801
(540) 434-5965
web site: **www.comsonics.com**
e-mail: **rschneid@shentel.net**

Ray Schneider has been the Director of Engineering at ComSonics since 1989 when he joined ComSonics from his position as Chief Scientist at Unisys's Washington Systems Engineering Center. Ray's team of engineers have developed many products for the CATV industry since that time including the Window Lite Plus, the Sniffer ID, the GeoSniffer, the Sleuth and others. Ray has a B.S. in Physics, an M.E. in Engineering Science and is completing his PhD in Information Technology at George Mason University. He is a licensed professional engineer in the state of Virginia.